

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION

FILED/ACCEPTED

OCT - 2 2009

Federal Communications Commission
Office of the Secretary

NBP-Public Notice #2

GN Docket Nos. 09-47, 09-51, 09-137

COMMENTS OF
CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC

October 2, 2009

No. of Copies of List ABCDE 044

CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC'S COMMENTS RESPONSIVE TO NBP-PUBLIC NOTICE #2

GN Docket Nos. 09-47, 09-51, 09-137

October 2, 2009

Overview of the Texas Electric Market

CenterPoint Energy Houston Electric, LLC ("CNP" or "Company") is a fully regulated transmission and distribution electric utility ("TDU") whose rates, operations, and services are subject to the jurisdiction of the Public Utility Commission of Texas ("PUC"). The structure of the Texas retail electric market is unique. Since 2002, electric utilities have been functionally unbundled with utility functions separated into the following three components: generation, transmission, and retail sales. Of these functions, only the transmission and distribution functions remain subject to utility regulation; the power generation, wholesale sale of electricity, and the retail electric sales functions now operate in a competitive marketplace.

As a result of this restructuring, a competitive market for retail electric services now exists in the Electric Reliability Council of Texas ("ERCOT") where retail consumers purchase electricity from among a large number of Retail Electric Providers ("REPs") that offer electricity at competitive prices with various service plans. In this environment, REPs purchase and schedule electricity from power generators based on their customers' expected usage, and TDUs like CNP deliver electricity from electric generating facilities to retail consumers for REPs in their respective service areas. CNP, for example, provides TDU delivery services for approximately 30 REPs that actively market electricity to residential consumers on the PUC's "The Power to Choose" website. REPs served by CNP currently serve over two million retail customers across a 5,000-square-mile area along the Texas Gulf Coast, including the Houston metropolitan area, the Nation's fourth largest city.

CenterPoint's Smart Grid Program

In this market environment, CNP has been authorized by the PUC to deploy an advanced metering system ("AMS") throughout its service area that will allow retail consumers to monitor and manage their electricity usage by having near real-time access to their electric usage in fifteen (15) minute increments. To provide this detailed usage information to retail consumers, CNP is constructing a robust data communications system and related back office systems as part of its deployment of advanced meters. It should be noted, however, that to make the Company's AMS cost-effective, CNP's core communications infrastructure has been designed to satisfy only the utility applications, such as AMS, that has been prescribed in the PUC approval order. To expand the communications network for other non-utility purposes would adversely impact current utility applications. The Company is also currently planning to install electric distribution grid automation equipment and technology, which will create an Intelligent Grid ("IG") and allow CNP to operate its distribution grid more efficiently, improve system reliability, and create the capability for the electric grid to "self-heal." Together, AMS and IG will form CNP's Smart Grid. The AMS data communications system will be an integral part of CNP's overall Smart Grid effort.

CenterPoint's Smart Grid Communication System

The communications network currently being implemented is a fundamental element of CNP's Smart Grid strategy. It is a bi-directional, high-speed communications infrastructure that is reliable, secure and scalable. The communication network components are adaptable to future technological advances through wireless remote firmware and software downloads. This network will employ high speed wireless links, Ethernet connections, microwave radio service, and fiber optic technologies to ensure the timely and adaptable information flow needed while complying with cyber security, interoperability, and technical standards. The infrastructure will serve as the communications backbone for the Company's Smart Grid, which consists of both the AMS and the IG systems.

The Smart Grid communications network will be a CNP-owned, private, point-to-multipoint infrastructure constituted of GE WiMax remote radios and base stations ("Take Out Points") communicating at 3.65 Gigahertz ("GHz"). This WiMax broadband wireless technology enables CNP to cover efficiently its service territory, which is a geographic area of 5,000 square miles. It also enables reliable Smart Grid communications across varying topography – heavily wooded areas, hills, and urban areas with tall buildings. Additionally, the WiMax protocol supports IP-based interoperability and advanced security (including AES-128 encryption, MAC and RADIUS authentication, VLAN tagging).

The communications system is being designed for appropriate throughput capacity and low latency ("high speed") to ensure scalability by supporting both immediate data flow for smart metering, and distribution and substation automation, but also the expected future increase in traffic, namely for Home Area Network ("HAN") messaging and ZigBee-enabled applications. High availability will be enabled via a combination of system redundancy and a secondary GPRS-based communications link. To withstand Houston's harsh weather--heat, humidity, and hurricanes--the system will be rugged and hosted in utility huts or weatherproof enclosures. Antenna specifications and mounting standards will be designed for high wind ratings.

Take Out Point radios will be strategically located at secured sites that have access to CNP's existing private operations network. Selected locations may consist of point-to-point microwave or fiber connection points, substations, transmission right-of-way, or CNP office locations. Remote radios will be co-located with the various Smart Grid devices, from smart meter data collectors ("Cell Relays") to IG controllers, RTUs, or automated switches.

Response to Specific Questions

1. Suitability of Communications Technologies. *Smart Grid applications are being deployed using a variety of public and private communications networks. We seek to better understand which communications networks and technologies are suitable for various Smart Grid applications.*

a. *What are the specific network requirements for each application in the grid (e.g., latency, bandwidth, reliability, coverage, others)?*

The Company's Smart Grid communications infrastructure consists of highly resilient technologies that are designed to carry data, including, *inter alia*, backhaul communications, to support all the

downstream networks for both the Company's transmission and distribution systems. This infrastructure may also be used for transmission protection and control schemes, which require minimal network latency. This infrastructure is composed largely of fiber optic and point-to-point licensed microwave networks with bandwidths ranging from Optical Carrier-3 (which is 155 Megabits per second ("Mbps")) to Optical Carrier-192 (which is 9.953 Gigabits per second ("Gbps")). Optical Carrier (or "OC") is a standardized set of specifications of transmission speeds utilized in the Synchronous Optical Network/Synchronous Digital Hierarchy ("SONET/SDH") telecommunications standard. A network must support restoration capabilities with redundant path, ring topologies as defined in the SONET/SDH standards. These networks are designed to support high reliability standards with minimal restoration periods.

The Wide Area Network ("WAN") extensions from the core communications infrastructure provide a communications path for Supervisory Control And Data Acquisition ("SCADA"), Distribution, and AMS data collection. WAN extension networks for the SCADA service and AMS have traditionally consisted of both leased line circuits and private point-to-multipoint licensed and unlicensed wireless networks. Utilities are using this existing infrastructure for multi-application support with a requirement for increased reliability. As a result, private wireless networks are viewed by many utilities as more reliable. Although WAN extension networks use Ethernet networking, it is important that they support the legacy SCADA devices through the serial protocols such as the Recommended Standard 232 (the standard for serial binary data signals) still commonly used today. We understand that many utilities indicate that nearly 80% of their field devices still require support of serial only connectivity. These networks are also designed to support high reliability standards with minimal restoration periods. The data transmission rates typically vary between 9.6Kbps (kilobits per second) to 4Mbps.

WAN extensions also support that portion of the Company's AMS which collect customer usage data from the hundreds and even thousands of metering collector points. Ethernet networking is the preferred means of transporting data across these networks. CNP has a proprietary communications system for customer usage data transmission from the individual customer meters to their respective data collection points. Private networks with proper design and technology selection may support a multi-application backhaul which, for CNP, supports both AMS meter networks and distribution automation.

The CNP requirement for Smart Grid network bandwidth is 2Mbps with a network latency requirement roundtrip of less than 30 msec.

If these differ by application, how do they differ?

No additional information submitted.

We welcome detailed Smart Grid network requirement analyses.

No additional information submitted.

b. *Which communications technologies and networks meet these requirements?*

Although wired solutions, including Broadband over Power Line (“BPL”), have been tested, wired solutions are not practical because of cost. Wireless communication technologies, such as WIMAX and microwave, also provide the most flexibility in deployment. This holds true for AMS, and even more so in a Distributed Automation (“DA”) environment where burying fiber or copper can be very costly and time-consuming. The Company’s core network infrastructure consists of fiber optics, point-to-multipoint WIMAX, and point-to-point microwave, which provide high-capacity bandwidth, recoverability, and reliability within the enterprise network. Due to the mission-critical applications that utilize these networks, this infrastructure is private to the utility.

Which are best suited for Smart Grid applications?

We believe that a private exclusive licensed broadband wireless system meets the needs for reliable Smart Grid applications.

If this varies by application, why does it vary and in what way?

No additional information submitted.

What are the relative costs and performance benefits of different communications technologies for different applications?

No additional information submitted.

c. *What types of network technologies are most commonly used in Smart Grid applications?*

Point-to-multipoint broadband/high bandwidth wireless communication is prevalent for AMS networks and WAN, as well as for Distributed Architecture (“DA”) applications. A point-to-point backhaul wireless solution in licensed frequencies provides high throughput that is not susceptible to communications interference.

We welcome detailed analysis of the costs, relative performance and benefits of alternative network technologies currently employed by existing Smart Grid deployments, including both “last mile,” backhaul, and control network technologies.

d. *Are current commercial communications networks adequate for deploying Smart Grid applications?*

After CNP reviewed commercial and private network options, we determined that the private structure best met our requirements.

If not, what are specific examples of the ways in which current networks are inadequate?

Five examples are security, reliability, coverage, repair response time, and availability, especially in emergency situations such as storms.

How could current networks be improved to make them adequate, and at what cost?

No additional information submitted.

If this adequacy varies by application, why does it vary and in what way?

No additional information submitted.

e. *How reliable are commercial wireless networks for carrying Smart Grid data (both in last-mile and backhaul applications)?*

Based on CNP's decision to utilize a private network, CNP is not responding to this and the following four questions.

Are commercial wireless networks suitable for critical electricity equipment control communications?

No response being provided.

How reliably can commercial wireless networks transmit Smart Grid data during and after emergency events?

No response being provided.

What could be done to make commercial wireless networks more reliable for Smart Grid applications during such events? No response being provided.

We welcome detailed comparisons of the reliability of commercial wireless networks and other types of networks for Smart Grid data transport.

No response being provided.

2. **Availability of Communications Networks.** *Electric utilities offer near universal service, including in many geographies where no existing suitable communications networks currently exist (for last-mile, aggregation point data backhaul, and utility control systems). We seek to better understand the availability of existing communications networks, and how this availability may impact Smart Grid deployments.*

a. *What percentage of electric substations, other key control infrastructure, and potential Smart Grid communications nodes have no access to suitable communications networks?*

A very high percentage, 90% or more, do not have suitable communications for Smart Grid applications. Suitable substation SCADA communications exist at all of CNP's substations. Approximately 2% of CNP's pole-top switches have SCADA sets and have a suitable wireless communication network.

What constitutes suitable communications networks for different types of control infrastructure?

Presently, a 19.2 kbps communication network is suitable for substation and pole-top switch SCADA applications. However, the upgrades to CNP's grid to be implemented as part of its Smart Grid will require an estimated 2 Mbps communication network.

We welcome detailed analyses of substation and control infrastructure connectivity, potential connectivity gaps, and the cost-benefit of different alternatives to close potential gaps.

No additional information submitted.

b. *What percentage of homes have no access to suitable communications networks for Smart Grid applications (either for last-mile, or aggregation point connectivity)?*

All AMS consumers in the CNP territory will have an equivalent and suitable communication network to support their advanced meter functionality. All CNP and other consumers in Texas will also have access to their near real time electricity usage via the Texas Common Portal, which is expected to be in operation in February 2010. Home Area Network ("HAN") functionality is expected to be available to consumers from their respective REPs through either the individual REP's communications systems or, to a lesser extent, via the utility communications network.

c. *In areas where suitable communications networks exist, are there other impediments preventing the use of these networks for Smart Grid communications?*

The main impediment is the lack of dedicated bandwidth. These existing networks already are burdened with payload/traffic, and the Smart Grid communications require a specific amount of bandwidth and throughput. Existing networks may not have the capacity to handle additional traffic, and a mechanism, such as Quality of Service, may be needed to prioritize traffic for Smart Grid's mission critical communications.

d. *How does the availability of a suitable broadband network (wireless, wireline or other) impact the cost of deploying Smart Grid applications in a particular geographical area?*

The communications network is a major investment that is a key consideration in the business case for Smart Grid. The communications network must have the capacity, security and flexibility to support the reliable operations of the power grid and be able to handle the large of amounts of data that a Smart Grid generates.

In areas with no existing networks, is this a major barrier to Smart Grid deployment?

CNP has chosen to utilize and to expand its existing communications network to implement its Smart Grid. Without such an existing network, the cost and technical requirements for creating a communications network from scratch could create a barrier to Smart Grid deployment..

We welcome detailed economic analyses showing how the presence (or lack) of existing communications networks impacts Smart Grid deployment costs.

CNP has estimated that the capital cost of its communications systems (including cell relays, GPRS, subscription services, and installation services) will be about \$99 million, which is approximately 16% of the total project capital cost of deploying its advanced metering system.

3. **Spectrum.** *Currently, Smart Grid systems are deployed using a variety of communications technologies, including public and private wireless networks, using licensed and unlicensed spectrum. We seek to better understand how wireless spectrum is or could be used for Smart Grid applications.*

a. *How widely used is licensed spectrum for Smart Grid applications (utility-owned, leased, or vendor-operated)?*

CNP is currently not using utility-owned, licensed spectrum for its Smart Grid applications because suitable leased spectrum is not available in our service area. Vendor-operated spectrum (700 MHz) offered by one vendor responding to our RFP was not selected primarily due to cost considerations.

For which applications is this spectrum used?

None, as stated above.

We welcome detailed analyses of current licensed spectrum use in Smart Grid applications, including frequencies and channels. No additional information submitted.

b *How widely used is unlicensed spectrum? For which applications is this spectrum used?*

For CNP, the unlicensed spectrum is the only spectrum available that is suitable. Unlicensed spectrum is attractive due to its higher bandwidth capability versus licensed spectrum. Utilities prefer the dedicated licensed spectrum, but small channel size availability has limited its use in higher bandwidth Ethernet applications. The frequency of 900 Megahertz ("MHZ") is commonly used for point-to-multipoint networks due to its long-range and better coverage requirements, which utilities require between monitoring or control points. The 2.4 Gigahertz ("GHz") frequency and the 5.8 GHz unlicensed have been used in some cases but do not offer the coverage that the 900 MHz frequency offers.

We welcome detailed analyses of current unlicensed spectrum use in Smart Grid applications, including frequencies and channels.

No additional information submitted.

c. *Have wireless Smart Grid applications using unlicensed spectrum encountered interference problems?*

Yes. Interference has been detected in the 3.65 GHz and 5.8 GHz bands and is being managed.

If so, what are the nature, frequency, and potential impact of these problems, and how have they been resolved?

When higher bandwidth is required, a larger channel size is required. The larger channel sizes are more susceptible to interference from other operators utilizing the same spectrum or band. When interference occurs, it results in increased latency due to the number of retries, and potential lost packets of data. To resolve this interference CNP is utilizing a narrower channel size at the cost of throughput. The 3.65 GHz to 3.70 GHz non-exclusive license band assists CNP in overcoming these issues but only in areas where there are no Fixed Service Satellites operating. Different vendors, e.g., satellite operators, provide specific radio features and functionalities to provide greater reliability within their network (e.g., channel size, frequency hopping, channel selection, and adjustable power output). In addition, use of specific antennas has minimized interference.

d. *What techniques have been successfully used to overcome interference problems, particularly in unlicensed bands?*

The primary methods to address radio frequency interference are spread-spectrum frequency hopping ("SSFH"), data error correction/detection, filtering, and antenna polarity choice. SSFH is a military process (declassified in the 1980's) designed to escape radio "jamming." In this process radios are configured to change their frequencies in a synchronized pattern to avoid destructive radio interference. Data transmission includes a cyclic-redundancy check ("CRC") algorithm for each block of data to check its integrity. When an error is detected, correction methods, such as an automatic retransmit request ("ARQ"), will repeat corrupted or missing information. Physical, electronic, and signal-processing filters may also be used to yield a narrower receiver channel to block interference near (but not on) the operational frequency. Finally, such physical methods as system-wide antenna polarity choice (similar to polarized sunglasses and photography filters to reduce sun glare) can be used to reduce interference on the adjacent polarity. However, these physical methods cannot reduce interference on the same polarity.

e. *Are current spectrum bands currently used by power utilities enough to meet the needs of Smart Grid communications?*

No, licensed spectrum bands for utilities that can meet the needs of Smart Grid communications do not exist. In areas where there is no Fixed Service Satellite (FSS) grandfathered operator, the 3.65 GHz -3.70 GHz band provides the necessary throughput to satisfy the technical requirements and requires coordination between the operators to reduce potential for interference. In areas where FSS grandfathered operators do exist, dedicated spectrum, such as that recently allocated by

Industry Canada (30 MHz in 1.8 GHz) would be extremely valuable, even in more remote areas where distance between links are greater, thus requiring lower frequency and higher power.

We welcome detailed studies and discussion showing that the current spectrum is or is not sufficient. No additional information submitted.

f. *Is additional spectrum required for Smart Grid applications?*

Yes.

If so, why are current wireless solutions inadequate?

The current licensed spectrum (900 MHz) that is available to power utilities for point-to-multipoint system has only narrow-bandwidth. Exclusive broadband licensed spectrum is needed.

(i.) *Coverage: What current and future nodes of the Smart Grid are not and will not be in the coverage area of commercial mobile operators or of existing utility-run private networks?*

CNP's existing private network covers all of CNP's electric service area; however, the network is narrow-bandwidth and not suitable for Smart Grid applications.

We welcome detailed descriptions of the location, number and connectivity required of each node not expected to be in coverage.

No additional information submitted.

(ii.) *Throughput: What is the expected throughput required by different communications nodes of the Smart Grid, today and in the future, and why will/won't commercial mobile networks and/or private utility owned networks on existing spectrum be able to support such throughputs?*

For today, 2 Mbps is required; in the future, over 10 Mbps is expected to be required. CNP does not have an existing privately owned network capable of meeting these requirements.

We welcome detailed studies on the location and throughput requirements and characteristics of each communications node in the Smart Grid.

Home Area Network ("HAN") throughput for Smart Grid reflects a utility grade service level and is not intended to compete with throughput serviceability normally associated with commercial providers. Because of data throughput limitations, simple text messaging, load controls, and price signaling latency through Smart Grid networks will be impacted when operating concurrently with normal utility business occurring over the same network. Even when utility transaction burden on the communications network is low, HAN communication latency will be slow compared to high speed broadband. Future HAN communication traffic levels are unknown, undefined, and are dependent on both consumer and service provider acceptance. HAN communications between the meter and in-home devices occur in near-real time.

(iii.) *Latency: What are the maximum latency limits for communications to/from different nodes of the Smart Grid for different applications, why will/won't commercial mobile networks be able to support such requirements, and how could private utility networks address the same challenge differently?*

Latency is crucial for requirements that are typically greater than 30 milliseconds ("msec"). To meet these requirements, the Company is designing and building its own network.

(iv.) *Security: What are the major security challenges, and the relative merits and deficiencies of private utility networks versus alternative solutions provided by commercial network providers, such as VPNs?*

Utilities are experienced in dealing with data privacy and security. CNP has fully considered and addressed cyber security concerns relating to its Smart Grid. As a TDU, the Company has extensive experience in administering cyber security protection on its bulk electric system. The ERCOT bulk power transmission grid uses a SCADA monitoring and control process to communicate. This is a fully automated system that permits continuous monitoring and control of the ERCOT grid and the generation attached to the grid. CNP has been an active participant in the development of NERC's cyber security standards and has fully implemented those standards for its transmission system. CNP's connection with the ERCOT bulk power transmission grid is through the CNP Control Center. The separation of the Control Center from the newly designed AMS program will ensure that there are no cyber security issues with AMS that could create problems for CNP's transmission system, the ERCOT bulk transmission system, or generation facilities connected to the grid. Thus, from an operational standpoint CNP has protected the bulk transmission grid from cyber attacks on the AMS by keeping complete separation between AMS and the Control Center.

The design of its Smart Grid also allows CNP to comply with future federal requirements and current/upcoming cyber security standards. The IG is being designed to comply with the NERC CIP Cyber Security Standards, which currently only apply to transmission level (bulk power) systems. The forward looking plan provides CNP with the confidence that future security requirements can be met without drastic changes to the system components or software systems that make up the IG. CNP has been a catalyst and an active advocate for national standards development and works with various industry groups to ensure the system is designed to meet future cyber security requirements. For example CNP is a key contributor to the GridWise Alliance, and a participant in EPRI Intelligrid R&D and the ZigBee Alliance.

In summary, CNP aggressively addresses cyber security in every phase of the engineering lifecycle of its Smart Grid, including design and procurement, installation and commissioning and the ability to provide ongoing maintenance and support. Cyber security solutions are deemed to be comprehensive and capable of being extended or upgraded in response to emerging cyber security threats or changes to the technological environment.

For all of these reasons, CNP did not select commercial networks that must be an integral part of our critical energy infrastructure.

Do the security requirements and the relative merits of commercial versus private networks depend on the specific Smart Grid application?

See the Company's response to Question 1(d) above.

If so, how?

No additional information submitted.

(v.) Coordination: Are there benefits or technical requirements to coordinate potential allocation of spectrum to the Smart Grid communications with other countries? What are they?

Although CNP's service territory is not located on the border with Mexico, the Company does believe that allocation of spectrum could minimize interference. The utilization of specified spectrum could also increase interoperability of devices, which could ultimately reduce costs.

(vi.) Spectrum allocation: Are there any specific requirements associated with Smart Grid communications that require or rule out any specific band, duplexing scheme (e.g., FDD vs TDD), channel width, or any other requirements or constraints?

CNP needs to provide coverage for approximately 5,000 square miles; therefore, the spectrum that is more suitable for operating over a long range and operating in forested areas is preferred.

g. If spectrum were to be allocated for Smart Grid applications, how would this impact current, announced and planned Smart Grid deployments?

If exclusive spectrum were allocated, CNP would use that spectrum for its Smart Grid program.

How many solutions would use allocated spectrum vs. current solutions? Which Smart Grid applications would likely be most impacted?

We believe that there would be a preference to use allocated spectrum. Both our AMS and IG programs would be impacted.

4. Real-time Data. *The Smart Grid promises to enable utility companies and their customers to reduce U.S. energy consumption using a variety of technologies and methods. Some of the most promising of these methods use demand response, in which utility companies can directly control loads within the home or business to better manage demand, or give price signals to encourage load shedding. Other methods reduce energy consumption simply by providing consumers access to their consumption information, via in-home displays, web portals, or other methods. Central to all of these techniques is energy consumption and pricing data.*

a. In current Smart Meter deployments, what percentage of customers have access to real-time consumption and/or pricing data? How is this access provided?

As of Dec. 31, 2009, CNP expects to have installed 145,000 meters and an additional 500,000 meters per year thereafter until approximately 2.2 million meters are installed to serve all the customers in the Company's service area. We are deploying Itron's OpenWay meter. These meters are equipped with ZigBee communication capability allowing users to securely link HAN devices to meters. Once linked, meters can provide HAN devices with near real time updates of electric consumption data; in OpenWay's case, this is every 7.5 seconds. Pricing data may be remotely transmitted to the meter or to HAN devices through the meter in compliance with ZigBee Smart Energy v1.0 specifications. After completion of the Texas Common Portal, CNP and Oncor consumers will be able to access 15-minute electricity consumption data on a day-after basis by logging onto the Texas Common Portal website and accessing their individual accounts.

b. *What are the methods by which consumers can access this data (e.g., via Smart Meter, via a utility website, via third-party websites, etc.)?*

There are several ways a consumer may access electricity usage data measured and collected by the Company's Smart Grid.

- **HAN** - In CNP's service area, consumers or service providers may "link" ZigBee Smart Energy profile HAN devices with the electric meter serving the individual consumer. Once linked, consumer access to usage data is based on the functionality of the HAN device. Typically, display devices provide data presentation options for numeric or graphic display and may include pricing calculators for converting actual usage into dollars and cents. The CNP Smart Grid meters require ZigBee Smart Energy version 1.0 specifications with Certicom Production Certificates to assure unique and secure links between the meter and a HAN device.
- **Texas Common Portal** – Retail consumers served by CNP and Oncor will be able to access their detailed energy usage and remotely access their HAN devices via the Texas Common Data Repository and Portal ("TCDRP"), which is currently being developed jointly by CNP and Oncor Electric Delivery Company. Other TDUs in ERCOT will have the opportunity to participate in this solution by making an appropriate financial commitment to cover the development and operation of the TCDRP.
- **REPs and 3rd Parties** - Consumers may also access Smart Grid data through websites offered by their individual REPs. CNP expects to see 3rd Party service offerings that leverage HAN communication for appliance monitoring and maintenance or other energy conservation or load management activities.

What are the relative merits and risks of each method?

Two key issues involved in providing consumer data are data security and latency. In Texas, consumers own their electric usage data. For this reason, access to an individual's data requires that individual customer's authorization. Both authentication and validation are must be provided to the regulated utility gathering the data in order for that individual to access the data. The availability of the data is a customer satisfaction matter, but may also impact demand response programs or a consumer's ability to timely react to price offerings.

- HAN provides consumers a local means of collecting usage information independent of a utilities Smart Grid network. Consumers will literally have access to their usage information well before the information may be collected by the utility. HAN devices also provide a means of executing demand response or load shaping functions, such as turning air conditioners, water heaters, pool pumps or any other large appliance on or off. Or, a consumer may “opt out” of a utility-controlled demand response or load shaping by issuing a command to a HAN device. HAN is an emerging technology with developing standards, developing security, and product availability issues.
- The Texas Common Portal will provide a secure means of accessing data. The data will initially be made available on a “day-after” basis.
- REPs and 3rd Party service providers may provide a range of data uses, presentations and service offerings, but they will be confined to Smart Grid data collection limitations. REPs and 3rd Parties may install “gateway” devices that provide both meter connectivity and 3rd Party broadband access. In this way, REPs and 3rd Party service providers may be capable of providing program functionality with short latency. However, consumers risk losing data privacy and security in such programs.

c. *How should third-party application developers and device makers use this data?*

Smart Grid opens the market for many imaginative applications based on granular consumer usage information. Consumers served by Smart Grid can use new service and product offerings capable of taking advantage of granular data availability. Thus, developers may want to target load shape management, conservation, time-sensitive pricing, pre-payment pricing, appliance maintenance and monitoring, remote appliance controls, PHEV charging/discharging monitoring and controls, renewable generation measurement, among others.

How can strong privacy and security requirements be satisfied without stifling innovation?

CNP’s advanced metering system includes a number of features designed to protect privacy and security. CNP believes failure to provide data security and privacy will stifle innovation as quickly as over burdening the market with security or privacy requirements. Smart Grid and Common Portal implementations such CNP’s and the Texas Common Portal properly balance security and privacy by leveraging security end-to-end and managing consumer data privacy as required by the PUCT. These features are built into CNP’s Smart Grid design and are practically invisible to consumers, although consumers will be required to grant authorization to parties requiring access to their data and grant permission to enable HAN device functionality.

d. *What uses of real-time consumption and pricing data have been shown most effective at reducing peak load and total consumption?*

Because CNP is limited to being the energy delivery utility, and not a retail electric provider, it will refrain from addressing this matter in detail. However, potential benefits of AMS are generally discussed in section (e) below.

We welcome detailed analyses of the relative merits and risks of these methods.

No additional information submitted.

- e. *Are there benefits to providing consumers more granular consumption data?*

The consumers will have significantly more data available concerning how much electricity they consume and when that consumption occurs. Consumer knowledge of their consumption patterns will facilitate more informed decisions concerning the management and conservation of electricity usage. When REPs begin offering Time of Use (“TOU”) rates structures, the increased knowledge on the part of consumers concerning their granular electricity usage should enable many consumers to reduce their electric usage. In addition, other consumers may be able to reduce their energy costs while using the same amount of electricity by shifting their usage from on-peak to off- peak periods.

We welcome studies that examine how consumer or business behavior varies with the type and frequency of energy consumption data.

No additional information submitted.

- f. *What are the implications of opening real-time consumption data to consumers and the energy management devices and applications they choose to connect?*

No additional information submitted.

5. **Home Area Networks.** *We seek to understand the ways in which utilities, technology providers and consumers will connect appliances, thermostats, and energy displays to each other, to the electric meter, and to the Internet.*

- a. *Which types of devices (e.g. appliances, thermostats, and energy displays, etc.) will be connected to Smart Meters?*

HAN devices provide either monitoring, display or control functionality. CNP requires a device to meet ZigBee Smart Energy specifications, version 1.0, with a Certicom Production Certificate to “link” with a CNP advanced meter. Once linked, depending on individual device capabilities, the device becomes part of the Smart Grid communication network. For example, a REP may send a load control message to the device through CNP’s Smart Grid or through 3rd Party broadband, or through both media. Any device meeting CNP’s connectivity requirements may “link” with CNP’s meter and either receive metered data, or participate in a communications network, or both.

CNP allows connections of five HAN devices to a meter. One or all of these devices may be gateway devices capable of connecting with other HAN devices. Gateway HAN devices may offer display and/or control functionality over an array of sub-devices. For example, a consumer may have usage and appliance monitoring devices connected to all major appliances which are connected to a central HAN control center that is “linked” to a meter. The control center displays the aggregated usage values recorded by the Smart Grid meter and the individual appliance usage values comprising the connected HAN grid. Appliance usage levels that exceed normal or reach

some pre-selected level are highlighted for the consumer's attention. Such central control centers may be HAN-equipped televisions.

What types of networking technologies will be used?

When fully developed, 3rd Party communications access to HAN devices will include cable, cellular telephone, internet, as well as through the Smart Grid itself.

What type of data will be shared between Smart Meters and devices?

Once connected to CNP's advanced meters, a two-way communication environment between the device and the meter is activated. HAN devices may receive a variety of data from the meter:

- interval electric usage information updated every 7.5 minutes,
- usage data history stored in meter memory,
- meter power status,
- communications connectivity status with the meter, and
- HAN messages from upstream systems, such as, load control signals, text messages, or pricing signals.

Depending on the HAN device, it may communicate acknowledgement of message receipt, a consumer's "opt out" action, or the operating status of the device.

b. *Which types of devices (e.g., appliances, thermostats, and energy displays, etc.) will be connected to the Internet?*

The company expects a rapidly growing offering of devices and services including those indicated in the question, as competing REPs and retail consumers adapt the energy management tools that will be available due to the deployment of the new AMS technology.

What types of networking technologies will be used?

The Texas Common Portal will be accessed by CNP and Oncor consumers using the Internet. The portal to the CNP data center will be a secure VPN tunnel or Texas market-approved encrypted batch data file transfer protocol. Once inside the CNP network, communications will be using an industry standard private network used only by CNP.

What type of data will be shared between these devices and the Internet?

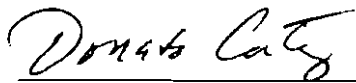
Usage data and limited results of HAN functionality that has been activated will be available to the consumer and other authorized parties.

c. *We welcome analyses that examine the role of broadband requirements for Home Area Networks that manage energy loads or deliver other energy management services.*

No additional information submitted.

Date: October 2, 2009

Respectfully submitted,

A handwritten signature in cursive script, reading "Donato Cortez".

Donato Cortez, Division Vice President
Regulated Operations Technology